In the Claims:

1. (Currently Amended) A system for network content monitoring, comprising:

a transport data monitor, connectable to a point in a network, for monitoring data being transported past said point,

a description extractor, associated with said transport data monitor, for extracting descriptions of said data being transported,

a database of at least one preobtained description of known content whose movements it is desired to monitor, said content being internally generated in the network in advance of said extracting, said preobtained description being obtained in advance of said extracting descriptions, and

a comparator, configured to determine whether said extracted description corresponds to any of said at least one preobtained descriptions, and to decide whether said data being transported comprises any of said content whose movements it is desired to monitor according to said determining.

2. (Original) A system according to claim 1, wherein said description extractor is operable to extract a pattern identifiably descriptive of said data being transported.

3. (Original) A system according to claim 1, wherein said description extractor is operable to extract a signature of said data being transported.

4. (Original) A system according to claim 1, wherein said description extractor is operable to extract characteristics of said data being transported.

5. (Original) A system according to claim 1, wherein said description extractor is operable to extract encapsulated meta information of said data being transported.

6. (Original) A system according to claim 1, wherein said description extractor is operable to extract multi-level descriptions of said data being transported.

7. (Original) A system according to claim 6, wherein said multi-level description comprises of a pattern identifiably descriptive of said data being transported.

8. (Original) A system according to claim 6, wherein said multi-level description comprises a signature of said data being transported.

9. (Original) A system according to claim 6, wherein said multi-level description comprises characteristics of said data being transported.

10. (Original) A system according to claim 6, wherein said multi-level description comprises encapsulated meta-information of said data being transported.

11. (Original) A system according to claim 1, wherein said description extractor is a signature extractor, for extracting a derivation of said data, said derivation being a signature indicative of content of said data being transported, and wherein said at least one preobtained description is a preobtained signature.

12. (Previously Presented) A system according to claim 1, said network being a packet-switched network and said data being transported comprising passing packets.

13. (Previously Presented) A system according to claim 1, said network being a packet-switched network, said data being transported comprising passing packets and said transport data monitor being operable to monitor header content of said passing packets.

14. (Previously Presented) A system according to claim 1, said network being a packet-switched network, said data being transported comprising passing packets, and said transport data extractor being operable to monitor header content and data content of said passing packets.

15. (Original) A system according to claim 1, wherein said transport data monitor is a software agent, operable to place itself on a predetermined node of said network.

16. (Original) A system according to claim 1, comprising a plurality of transport data monitors distributed over a plurality of points on said network.

17. (Original) A system according to claim 1, said transport data monitor further comprising a multimedia filter for determining whether passing content comprises multimedia data and restricting said signature extraction to said multimedia data.

18. (Original) A system according to claim 1, said data being transported comprising a plurality of protocol layers, the system further comprising a layer analyzer connected between said transport data monitor and said signature extractor, said layer analyzer comprising analyzer modules for at least two of said layers.

19. (Original) A system according to claim 18, said layer analyzer comprising separate analyzer modules for respective layers.

20. (Original) A system according to claim 18, further comprising a traffic associator, connected to said analyzer modules, for using output from said analyzer modules to associate transport data from different sources as a single communication.

21. (Original) A system according to claim 20, wherein said sources are at least one of a group comprising: data packets, communication channels, data monitors, and pre correlated data.

22. (Original) A system according to claim 18, comprising a traffic state associator connected to receive output from said layer analyzer modules, and to associate together output, of different layer analyzer modules, which belongs to a single communication.

23. (Original) A system according to claim 18, wherein at least one of said analyzer modules comprises a multimedia filter for determining whether passing content comprises multimedia data and restricting said signature extraction to said multimedia data.

24. (Original) A system according to claim 18, wherein at least one of said analyzer modules comprises a compression detector for determining whether said extracted transport data is compressed.

25. (Original) A system according to claim 24, further comprising a decompressor, associated with said compression detector, for decompressing said data if it is determined that said data is compressed.

26. (Original) A system according to claim 24, further comprising a description extractor for extracting a description directly from said compressed data.

27. (Original) A system according to claim 18, wherein at least one of said analyzer modules comprises an encryption detector for determining whether said transport data is encrypted.

28. (Original) A system according to claim 27, wherein said encryption detector comprises an entropy measurement unit for measuring entropy of said monitored transport data.

29. (Original) A system according to claim 28, wherein said encryption detector is set to recognize a high entropy as an indication that encrypted data is present.

30. (Original) A system according to claim 29, wherein said encryption detector is set to use a height of said measured entropy as a confidence level of said encrypted data indication.

31. (Original) A system according to claim 18, further comprising a format detector for determining a format of said monitored transport data.

32. (Original) A system according to claim 31, further comprising a media player, associated with said format detector, for rendering and playing said monitored transport data as media according to said detected format, thereby to place said monitored transport data in condition for extraction of a signature which is independent of a transportation format.

33. (Original) A system according to claim 31, further comprising a parser, associated with said format detector, for parsing said monitored transport media, thereby to place said monitored transport data in condition for extraction of a signature which is independent of a transportation format.

34. (Original) A system according to claim 1, comprising a payload extractor located between said transport monitor and said signature extractor for extracting content carrying data for signature extraction.

35. (Original) A system according to claim 1, wherein said signature extractor comprises a binary function for applying to said monitored transport data.

36. (Original) A system according to claim 1, wherein said network is a packet network, and wherein a buffer is associated with said signature extractor to enable said signature extractor to extract a signature from a buffered batch of packets.

37. (Original) A system according to claim 35, wherein said binary function comprises at least one hash function.

38. (Original) A system according to claim 37, wherein said binary function comprises a first, fast, hash function to identify an offset in said monitored transport data and a second, full, hash function for application to said monitored transport data using said offset.

39. (Original) A system according to claim 11, wherein said signature extractor comprises an audio signature extractor for extracting a signature from an audio part of said monitored data being transported.

40. (Original) A system according to claim 11, wherein said signature extractor comprises a video signature extractor for extracting a signature from a video part of said monitored data being transported.

41. (Original) A system according to claim 11, said signature extractor comprising a pre-processor for pre-processing said monitored data being transported to improve signature extraction.

42. (Original) A system according to claim 41, said preprocessor operable to carry out at least one of a group of pre-processing operations comprising: removing erroneous data, removing redundancy, and canonizing properties of said monitored data being transported.

43. (Original) A system according to claim 11, wherein said signal extractor comprises a binary signal extractor for initial signature extraction and an audio signature extractor for extracting an audio signature in the event said initial signature extraction fails to yield an identification.

44. (Original) A system according to claim 11, wherein said signal extractor comprises a binary signal extractor for initial signature extraction and a text signature extractor for extracting a text signature in the event said initial signature extraction fails to yield an identification.

45. (Original) A system according to claim 11, wherein said signal extractor comprises a binary signal extractor for initial signature extraction and a code signature extractor for extracting a code signature in the event said initial signature extraction fails to yield an identification.

46. (Original)A system according to claim 11, wherein said signal extractor comprises a binary signal extractor for initial signature extraction and a data content signature extractor for extracting a data content signature in the event said initial signature extraction fails to yield an identification.

47. (Original) A system according to claim 11, wherein said signature extractor is operable to use a plurality of signature extraction approaches.

48. (Original) A system according to claim 47, further comprising a combiner for producing a combination of extracted signatures of each of said approaches.

49. (Original) A system according to claim 47, wherein said comparator is operable to compare using signatures of each of said approaches and to use as a comparison output a highest result of each of said approaches.

50. (Original) A system according to claim 11, wherein said signal extractor comprises a binary signal extractor for initial signature extraction and a video signature extractor for extracting a video signature in the event said initial signature extraction fails to yield an identification.

51. (Original) A system according to claim 11, wherein there is a plurality of preobtained signatures and wherein said comparator is operable to compare said extracted signature with each one of said preobtained signatures, thereby to determine whether said monitored transport data belongs to a content source which is the same as any of said signatures.

52. (Original) A system according to claim 51, said comparator being operable to obtain a cumulated number of matches of said extracted signature.

53. (Original) A system according to claim 51, wherein said comparator is operable to calculate a likelihood of compatibility with each of said preobtained signatures and to output a highest one of said probabilities to an unauthorized content presence determinator connected subsequently to said comparator.

54. (Original) A system according to claim 52, said comparator being operable to calculate a likelihood of compatibility with each of said preobtained signatures and to output an accumulated total of matches which exceed a threshold probability level.

55. (Original) A system according to claim 52, said comparator being operable to calculate the likelihood of compatibility with each of said preobtained signatures and to output an accumulated likelihood of matches which exceed a threshold probability level.

56. (Original) A system according to claim 51, comprising a sequential decision unit associated with said comparator, being operable to use a sequential decision test to update a likelihood of the presence of given content, based on at least one of the following: successive matches made by said comparator, context related parameters, other content related parameters and outside parameters.

57. (Original) A system according to claim 53, wherein said unauthorized content presence determinator is operable to use the output of said comparator to determine whether unauthorized content is present in said transport and to output a positive decision of said presence to a subsequently connected policy determinator.

58. (Original) A system according to claim 51, wherein an unauthorized content presence determinator is connected subsequently to said comparator and is operable to use an output of said comparator to determine whether unauthorized content is present in said data being transported, a positive decision of said presence being output to a subsequently connected policy determinator.

59. (Original) A system according to claim 58, wherein said policy determinator comprises a rule-based decision making unit for producing an enforcement decision based on output of at least said unauthorized content presence determinator.

60. (Original) A system according to claim 1, wherein said policy determinator is operable to use said rule-based decision making unit to select between a set of outputs including at least some of: taking no action, performing auditing, outputting a transcript of said content, reducing bandwidth assigned to said transport, using an active bitstream interference technique, stopping said transport, preventing printing, preventing photocopying, reducing quality of the content, removing sensitive

parts, altering the content, adding a message to the said content, and preventing of saving on a portable medium,

61. (Original) A system according to claim 60, wherein said rule-based decision making unit is operable to use a likelihood level of a signature identification as an input in order to make said selection.

62. (Original) A system according to claim 61, further comprising a bandwidth management unit connected to said policy determinator for managing network bandwidth assignment in accordance with output decisions of said policy determinator.

63. (Original) A system according to claim 1, further comprising an audit unit for preparing and storing audit reports of transportation of data identified as corresponding to content it is desired to monitor.

64. (Original) A system according to claim 1, comprising a transcript output unit for producing transcripts of content identified by said comparison.

65. (Original) A system according to claim 27, further comprising a policy determinator connected to receive outcomes of said encryption determinator and to apply rule-based decision making to select between a set of outputs including at least some of: taking no action, performing auditing, outputting a transcript of said content, reducing bandwidth assigned to said transport, using an active bitstream interference technique, and stopping said transport.

66. (Original) A system according to claim 65, wherein said rule-based decision-making comprises rules based on confidence levels of said outcomes.

67. (Original) A system according to claim 65, wherein said policy determinator is operable to use an input of an amount of encrypted transport from a given user as a factor in said rule based decision making.

68. (Original) A system according to claim 30, further comprising a policy determinator connected to receive positive outcomes of said encryption determinator and to apply rule-based decision making to select between a set of outputs including at least some of: taking no action, performing auditing, outputting a transcript of said content, reducing bandwidth assigned to said transport, using an active bitstream interference technique, and stopping said transport, said policy determinator operable to use:

an input of an amount of encrypted transport from a given user, and

said confidence level, as factors in said rule based decision making.

69. (Currently Amended) A system for network content control, comprising:

a transport data monitor, connectable to a point in a network, for monitoring data being transported past said point,

a signature extractor, associated with said transport data monitor, for extracting a derivation of payload of said monitored data, said derivation being indicative of content of said data,

a database of preobtained signatures of known content whose movements it is desired to monitor, said content being internally generated in the network in advance of said extracting, said preobtained signatures being obtained in advance of said extracting asaid derivation of said payload,

a comparator for comparing said derivation with said preobtained signatures, and to determine whether said monitored data comprises any of said content whose movements it is desired to control,

a decision-making unit for producing an enforcement decision, using the output of said comparator, and

a bandwidth management unit connected to said decision-making unit for managing network bandwidth assignment in accordance with output decisions of said policy determinator, thereby to control content distribution over said network.

70. (Original) A system according to claim 69, wherein said decision-making unit is a rule-based decision-making unit.

71. (Original) A system according to claim 70, wherein said transport data monitor is a software agent, operable to place itself on a predetermined node of said network.

72. (Original) A system according to claim 70, comprising a plurality of transport data monitors distributed over a plurality of points on said network.

73. (Original) A system according to claim 70, said transport data monitor further comprising a multimedia filter for determining whether passing content comprises multimedia data and restricting said signature extraction to said multimedia data.

74. (Original) A system according to claim 70, said transport data comprising a plurality of protocol layers, the system further comprising a layer analyzer connected between said transport data monitor and said signature extractor, said layer analyzer comprising analyzer modules for at least two of said layers.

75. (Original) A system according to claim 74, comprising a traffic state associator connected to receive output from said layer analyzer modules, and to associate together output of different layer analyzer modules which belongs to a single communication.

76. (Original) A system according to claim 74, one of said analyzer modules comprising a multimedia filter for determining whether passing content

comprises multimedia data and restricting said data extraction to said multimedia data.

77. (Original) A system according to claim 74, one of said analyzer modules comprising a compression detector for determining whether said monitored transport data is compressed.

78. (Original) A system according to claim 77, further comprising a decompressor, associated with said compression detector, for decompressing said data if it is determined that said data is compressed.

79. (Original) A system according to claim 74, one of said analyzer modules comprising an encryption detector for determining whether said monitored transport data is encrypted.

80. (Original) A system according to claim 79, wherein said encryption detector comprises an entropy measurement unit for measuring entropy of said monitored transport data.

81. (Original) A system according to claim 80, said encryption detector being set to recognize a high entropy as an indication that encrypted data is present.

82. (Original) A system according to claim 81, said encryption detector being set to use a height of said measured entropy as a confidence level of said encrypted data indication.

83. (Original) A system according to claim 74, further comprising a format detector for determining a format of said monitored transport data.

84. (Original) A system according to claim 83, further comprising a media player, associated with said format detector, for rendering and playing said monitored transport data as media according to said detected format, thereby to place said extracted transport data in condition for extraction of a signature which is independent of a transportation format.

85. (Original) A system according to claim 83, further comprising a parser, associated with said format detector, for parsing said monitored transport media, thereby to place said extracted transport data in condition for extraction of a signature which is independent of a transportation format.

86. (Original) A system according to claim 70, wherein said signature extractor comprises a binary function for applying to said extracted transport data.

87. (Original) A system according to claim 86, wherein said binary function comprises at least one hash function.

88. (Original) A system according to claim 87, wherein said binary function comprises a first, fast, hash function to identify an offset in said extracted transport data and a second, full, hash function for application to said extracted transport data using said offset.

89. (Original) A system according to claim 70, wherein said signature extractor comprises an audio signature extractor for extracting a signature from an audio part of said extracted transport data.

90. (Original) A system according to claim 70, wherein said signature extractor comprises a video signature extractor for extracting a signature from a video part of said extracted transport data.

91. (Original) A system according to claim 70, wherein said comparator is operable to compare said extracted signature with each one of said preobtained signatures, thereby to determine whether said monitored transport data belongs to a content source which is the same as any of said signatures.

92. (Original) A system according to claim 91, wherein said comparator is operable to calculate a likelihood of compatibility with each of said preobtained signatures and to output a highest one of said probabilities to an unauthorized content presence determinator connected subsequently to said comparator.

93. (Original) A system according to claim 92, wherein said unauthorized content presence determinator is operable to use the output of said comparator to determine whether unauthorized content is present in said transport and to output a positive decision of said presence to a subsequently connected policy determinator.

94. (Original) A system according to claim 91, wherein an unauthorized content presence determinator is connected subsequently to said comparator and is operable to use an output of said comparator to determine whether unauthorized content is present in said transport, a positive decision of said presence being output to a subsequently connected policy determinator.

95. (Original) A system according to claim 94, wherein said policy determinator comprises said rule-based decision making unit for producing an enforcement decision based on output of at least said unauthorized content presence determinator.

96. (Original) A system according to claim 70, wherein said policy determinator is operable to use said rule-based decision making unit to select between a set of outputs including at least some of: taking no action, performing auditing, outputting a transcript of said content, reducing bandwidth assigned to said transport, using an active bitstream interference technique, stopping said transport, not allowing printing of said content, not allowing photocopying of said content and not allow saving of said content on portable media.

97. (Original) A system according to claim 96, said rule-based decision making unit is operable to use a likelihood of a signature identification as an input in order to make said selection.

98. (Original) A system according to claim 70, further comprising an audit unit for preparing and storing audit reports of transportation of data identified as corresponding to content it is desired to monitor.

99. (Original) A system according to claim 79, further comprising a policy determinator connected to receive positive outcomes of said encryption determinator and to apply rule-based decision of said rule-based decision making unit to select between a set of outputs including at least some of: taking no action, performing auditing, outputting a transcript of said content, reducing bandwidth assigned to said transport, using an active bitstream interference technique, stopping said transport, reducing quality of the content, removing sensitive parts, altering the content, adding a message to said content, not allowing printing of said content, not allowing photocopying of said content and not allow saving of said content on portable media.

100. (Original) A system according to claim 99, said policy determinator being operable to use an input of an amount of encrypted transport from a given user as a factor in said rule based decision making.

101. (Original) A system according to claim 82, further comprising a policy determinator connected to receive positive outcomes of said encryption determinator and to apply rule-based decision making of said rule-based decision-making unit to select between a set of outputs including at least some of: taking no action, performing auditing, outputting a transcript of said content, reducing bandwidth assigned to said transport, using an active bitstream interference technique, stopping said transport, reducing quality of the content, removing sensitive parts, altering the content, adding a message to said content, not allowing printing of said content, not allowing photocopying of said content, and not allowing saving of said content on portable media.

102. (Original) A system according to claim 101, said policy determinator being operable to use:

an input of an amount of encrypted transport from a given user, and

said confidence level,

as factors in said rule based decision making.

103. (Original) A system according to claim 69, comprised within a firewall.

104. (Original) A system according to claim 103, said transport data monitor being operable to inspect incoming and outgoing data transport crossing said firewall.

105. (Original) A system according to claim 69, operable to define a restricted network zone within said network by inspecting data transport outgoing from said zone.

106. (Original) A system according to claim 69, comprising certification recognition functionality to recognize data sources as being trustworthy and to allow data transport originating from said trustworthy data sources to pass through without monitoring.

107. (Original) A system according to claim 69, comprising certification recognition functionality to recognize data sources as being trustworthy and to allow data transport originating from said trustworthy data sources to pass through with monitoring modified on the basis of said data source recognition.

108. (Original) A system according to claim 69, comprising certification recognition functionality to recognize data sources as being trustworthy and to allow data transport originating from said trustworthy data sources to pass through with said decision making being modified on the basis of said data source recognition.

109. (Currently Amended) A method of monitoring for distribution of known sensitive content over a network, the method comprising:

obtaining extracts of data from at least one monitoring point on said network,

obtaining a signature indicative of content of said extracted data,

comparing said signature with at least one of a set of signatures indicative of the sensitive content, said sensitive content being internally generated in the network in advance of said obtaining extracts, said set of signatures being stored in advance of said obtaining extracts of data,

determining if said extracted data comprises any of said sensitive content according to said comparing, and

using an output of said determining as an indication of the presence or absence of the sensitive content.

110. (Currently Amended) A method of controlling the distribution of known sensitive content over a network, the method comprising:

obtaining extracts of data from at least one monitoring point on said network,

obtaining a signature indicative of content of said extracted data,

comparing said signature with at least one of a set of signatures indicative of the ~~sensitive~~ presence of the sensitive content, said set being stored in advance of said obtaining extracts of data, said sensitive content being internally generated in the network in advance of said obtaining extracts,

determining if said extracted data comprises any of said sensitive content according to said comparing,

using an output of said determining in selecting an enforcement decision, and

using said enforcement decision in bandwidth management of said network.

111. (Original) A method according to claim 110, wherein enforcement decisions for selection include at least some of taking no action, performing auditing,

outputting a transcript of said content, reducing bandwidth assigned to said transport, stopping said transport, reducing quality of the content, removing sensitive parts, altering the content, adding a message to said content, using an active bitstream interference technique, restricting bandwidth to a predetermined degree, not allowing printing of said content, not allowing photocopying of said content and not allowing saving of said content on portable media.

112. (Original) A method according to claim 111, wherein said predetermined degree is selectable from a range extending between minimal restriction and zero bandwidth.

113. (Previously Presented) A system according to claim 1, wherein said transport data monitor comprises functionality to remove steganograms, said steganograms for removal being steganograms comprising information hidden within said data being monitored by said transport data monitor.

114. (Previously Presented) A system according to claim 113, wherein said functionality to remove steganograms is independent of at least one of a group comprising:

a content of said steganogram hidden within said data being monitored,

a content of said information hidden within said data being monitored, and

of a method of hiding of said steganogram within said data being monitored.

115. (Previously Presented) A system according to claim 69, wherein said functionality to remove steganograms comprises at least one of the following:

adding noise to said data being monitored by said transport data monitor;

distorting said data being monitored by said transport data monitor; and

embedding at least one steganogram within said data being monitored by said transport data monitor.

116. (Previously Presented) A system according to claim 69, wherein said transport data monitor comprises functionality to remove steganograms, said steganograms for removal being steganograms comprising information hidden within said data being monitored by said transport data monitor.

117. (Previously Presented) A system according to claim 116, wherein said functionality to remove steganograms is independent of at least one of a group comprising:

a content of said steganogram hidden within said data being monitored,

a content of said information hidden within said data being monitored, and

of a method of hiding of said steganogram within said data being monitored.

118. (Previously Presented) A system according to claim 116, wherein said functionality to remove steganograms comprises at least one of the following:

adding noise to said data being monitored by said transport data monitor;

distorting said data being monitored by said transport data monitor; and

embedding at least one steganogram within said data being monitored by said transport data monitor.

119. (Previously Presented) A method according to claim 109, further comprising removing steganograms from said extracted data, said steganograms being hidden within said data.

120. (Previously Presented) A method according to claim 119, wherein said removing steganograms is independent of at least one of a group comprising:

a content of said steganogram hidden within said data,

a content of said information hidden within said data, and

of a method of hiding of said steganogram within said data.

121. (Previously Presented) A method according to claim 119, wherein said removing steganograms comprises at least one of the following:

adding noise to said data;

distorting said data; and

embedding at least one further steganogram within said data.

122. (Previously Presented) A method according to claim 110, further comprising removing steganograms from said extracted data, said steganograms being hidden within said data.

123. (Previously Presented) A method according to claim 122, wherein said removing steganograms is independent of at least one of a group comprising:

a content of said steganogram hidden within said data,

a content of said information hidden within said data, and

of a method of hiding of said steganogram within said data.

124. (Previously Presented) A method according to claim 122, wherein said removing steganograms comprises at least one of the following:

adding noise to said data;

distorting said data; and

embedding at least one further steganogram within said data.

125. (New) A system for network content monitoring, comprising:

a transport data monitor, connectable to a point in a network, for monitoring data being transported past said point,

a description extractor, associated with said transport data monitor, for extracting descriptions of said data being transported,

a database of at least one preobtained description of known prepossessed content whose movements it is desired to monitor, said preobtained description being obtained in advance of said extracting descriptions, and

a comparator, configured to determine whether said extracted description corresponds to any of said at least one preobtained descriptions, and to decide whether said data being transported comprises any of said prepossessed content whose movements it is desired to monitor according to said determining.

126. (New) A system for network content monitoring, comprising:

a transport data monitor, connectable to a point in a network, for monitoring data being transported past said point,

a description extractor, associated with said transport data monitor, for extracting descriptions of said data being transported,

a database of at least one preobtained description of known content whose movements it is desired to monitor, said content never sent out of the network, said content being internally generated in the network in advance of said extracting, said preobtained description being obtained in advance of said extracting descriptions, and

a comparator, configured to determine whether said extracted description corresponds to any of said at least one preobtained descriptions, and to decide whether said data being transported comprises any of said content whose movements it is desired to monitor according to said determining.